

**UNITED STATES DISTRICT COURT  
NORTHERN DISTRICT OF NEW YORK**

---

**UNITED STATES OF AMERICA,**

**v.**

**1:20-CR-335 (TJM)**

**JACOB DELANEY,**

**Defendant.**

---

**THOMAS J. McAVOY,  
Senior United States District Judge**

**SEALED DECISION and ORDER<sup>1</sup>**

**I. INTRODUCTION**

Defendant Jacob Delaney was indicated on one count of receiving child pornography in violation of 18 U.S.C. §§ 2252A(a)(2)(A) and (b)(1), and three counts of possessing child pornography in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). See Dkt. No. 29. Defendant moves to suppress all physical evidence seized from his residence, computers, and electronic storage media pursuant to a search warrant issued by the Hon. Daniel J. Stewart, United States Magistrate Judge, and to suppress all statements obtained during and after the search. See Dkt. Nos. 43, 44, 46-1 and 46-2 at 1.

---

<sup>1</sup>The Government was granted protective orders covering the search warrant application and affidavit, and covering certain discovery material provided by the government. See Dkt. Nos. 22, 38. The bases for the protective orders are that the information covered by the protective orders purportedly concerned sensitive information related to the ongoing investigations of investigative targets suspected of engaging in online child sexual exploitation, the dissemination of which the Government asserts could seriously jeopardize those continuing investigations.

Defendant primarily presents two arguments challenging the probable cause determination on the warrant. He argues that there was insufficient evidence demonstrating that his IP address accessed the website in question ("Target Website"), contending that law enforcement can only identify his IP address as one of many possible IP addresses involved in the relay of information to and from the Target Website. Dkt. Nos. 44 (Def. redacted Mem. L.), at 1; 46-2 (Def. sealed Mem. L.) at 1. He also contends that even if the evidence demonstrates that his IP address accessed the Target Website, the evidence at most demonstrates a single alleged visit of an unknown duration to the Target Website seven and a half months before the warrant was sought. *Id.* Defendant argues that the facts underlying the warrant application are independently deficient and stale, contending that the allegations in the supporting affidavit are insufficient to support probable cause to believe that evidence of criminality could be found at his residence, on his computers, or on his electronic storage media. *Id.* at 7. He also argues that the good-faith exception to the exclusionary rule does not apply because "the applying agent demonstrated gross negligence by ignoring clearly established Second Circuit search and seizure law; the application so lacked indicia of probable cause that it was unreasonable to rely upon it; and the applying agent recklessly provided misleading information to the reviewing magistrate by failing to include critical facts and making unsupported conclusions about the likelihood that evidence of criminality would be found at the location to be searched." *Id.* at 1. Defendant argues that as a consequence, all evidence obtained from the search must be suppressed. *Id.* In addition, Defendant contends that all statements he made on the date the warrant was executed, even those that followed

*Miranda* warnings, should be suppressed as they are the product of the government's unlawful search and seizure and are not attenuated in time or place to the Fourth Amendment violation such to remove the taint from the unlawful search. *Id.* at 14.

The Government opposes the motion, arguing that sufficient probable cause existed and, even if it did not, the good-faith exception to the exclusionary rule applies. See Dkt. Nos. 51-1 (Gov. redacted Mem. L. in Opp.), 53 (Gov. sealed Mem. L. in Opp.). The Government also argues that Defendant's non-custodial and post-*Miranda* admissions that were given during and after the execution of a valid search warrant should not be suppressed. *Id.*

## **II. BACKGROUND**

### **a. Search Warrant**

On December 10, 2019, Judge Stewart authorized a federal "no knock" Search and Seizure Warrant to search Defendant's residence ("the Subject Premises") located in New Paltz, New York, Defendant's person, and any computers and electronic storage media located during those searches, and to seize evidence, fruits and instrumentalities of violations of 18 U.S.C. §§ 2252A(5)(B) and (b)(2), possessing or accessing with the intent to view child pornography and attempt or conspiracy to do the same. See Def. Ex. F, Dkt. No. 46-7 (filed under seal). Judge Stewart based his determination on the facts and information provided in an application and affidavit sworn to by FBI Special Agent David Fallon ("SA Fallon"). See Def. Ex. E, Dkt. No. 46-6 (filed under seal).

SA Fallon's affidavit indicates that the government's investigation concerns alleged violations of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2), which prohibits any person from



knowingly possessing or accessing with the intent to view, or attempting or conspiring to possess or access with the intent to view, child pornography. Dkt. 46-6 at ¶ 4. After providing relevant definitions for some words and phrases used in the affidavit, *id.* at ¶ 5(a)-(t), SA Fallon then addresses the background of the investigation and the facts that he believed constituted probable cause for the warrant. He indicates that “[a] user of the Internet account at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on the Tor anonymity network.<sup>2</sup> The website is described below and referred to herein as ‘TARGET WEBSITE.’ There is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed TARGET WEBSITE, as further described herein.” *Id.* at ¶ 6.

### **The Tor Network**

SA Fallon describes the Tor network as follows:

7. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are uniquely identified by IP addresses, which are used to route information between Internet-connected devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. On the Internet, data transferred between devices is split into discrete packets, each of which has two parts: a header with non-content routing and control information, such as the packet's source and destination IP addresses; and a payload, which generally contains user data or the content of a communication.

8. The website further described below operated on the Tor network, which is a computer network available to Internet users that is designed specifically

---

<sup>2</sup>As the Second Circuit recognized in another case, “‘The Onion Router’ (better known as ‘Tor’), [is] an ‘anonymizing network’ that allows users who have downloaded the Tor software to access websites without revealing their IP addresses or other identifying information by routing their internet traffic through numerous relay computers located around the world before such traffic arrives at a desired web location.” *United States v. Eldred*, 933 F.3d 110, 112 (2d Cir. 2019).



to facilitate anonymous communication over the Internet. The Tor network attempts to do this by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a "circuit." Because of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective.

9. To access the Tor network, a user must install Tor software. That is most easily done by downloading the free "Tor browser" from the Tor Project, the private entity that maintains the Tor network, via their website at [www.torproject.org](http://www.torproject.org).<sup>3</sup> The Tor browser is a web browser that is configured to route a user's Internet traffic through the Tor network.

10. As with other Internet communications, a Tor user's communications are split into packets containing header information and a payload, and are routed using IP addresses. In order for a Tor user's communications to be routed through the Tor network, a Tor user necessarily (and voluntarily) shares the user's IP address with Tor network relay computers, which are called "nodes." This routing information is stored in the header portion of the packet. As the packets travel through the Tor network, each node is able to see the address information of the previous node the communication came from and the next node the information should be sent to. Those Tor nodes are operated by volunteers - individuals or entities who have donated computers or computing power to the Tor network in order for it to operate.

11. Because a Tor user's communications are routed through multiple nodes before reaching their destination, when a Tor user accesses an Internet website, only the IP address of the last relay computer (the "exit node"), as opposed to the Tor user's actual IP address, appears on that website's IP address log. In addition, the content of a Tor user's communications are encrypted while the communication passes through the Tor network. That can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications.

12. The Tor Project maintains a publicly available frequently asked questions (FAQ) page, accessible from its website, with information about the Tor network. Within those FAQ, the Tor Project advises Tor users that the first Tor relay to which a user connects can see the Tor user's actual IP address. In addition, the FAQ also cautions Tor users that the use of the Tor network does not render a user's communications totally anonymous. For example, in the Tor Project's FAQ, the question "So I'm totally anonymous if I use Tor?"

---

<sup>3</sup>SA Fallon's affidavit includes this footnote: "Tor users may also choose to manually configure a web browser or other application to route communications through the Tor network."

is asked, to which the response is, in bold text, "No."

13. The Tor Network also makes it possible for users to operate websites, such as those described herein, called "hidden services" or "onion services," in a manner that attempts to conceal the true IP address of the computer hosting the website. Hidden service websites are accessible only to users operating within the Tor network. Like other websites, hidden services are hosted on computer servers that communicate through IP addresses. However, hidden services have unique technical features that attempt to conceal the computer server's location.

14. Unlike standard Internet websites, a Tor-based web address is comprised of a series of at least 16 and as many as 56 algorithm-generated characters, for example "asdlk8fs9dfiku7f," followed by the suffix ".onion." Ordinarily, investigators can determine the IP address of the computer server hosting a website (such as www.justice.gov) by simply looking it up on a publicly available Domain Name System ("DNS") listing. Unlike ordinary Internet websites, however, there is no publicly available DNS listing through which one can query the IP address of a computer server that hosts a Tor hidden service. So, while law enforcement agents can often view and access hidden services that are facilitating illegal activity, they cannot determine the IP address of a Tor hidden service computer server via public lookups. Additionally, as with all Tor communications, communications between users' computers and a Tor hidden service webserver are routed through a series of intermediary computers. Accordingly, neither law enforcement nor hidden-service users can use public lookups or ordinary investigative means to determine the true IP address - and therefore the location - of a computer server that hosts a hidden service.

Dkt. 46-6 at ¶¶ 7-14 (footnote in original).

### **The Target Website**

SA Fallon next describes the "Target Website" as follows:

15. The conduct being investigated involves users of a Tor-network-based website (hereinafter "TARGET WEBSITE") that functioned as an active online forum whose primary purpose was to be a board that was "public, open and free, however, slightly moderate(d) to avoid things that are harmful to the community and/or members, here you can be happy, be yourself and can talk about anything, even controversial issues, but always respecting the rights of other members." The website was dedicated to the sexual exploitation of minor and/or prepubescent males. The advertisement and distribution of child pornography and child erotica were regular occurrences on this site. The website launched in approximately 2013 and ceased



operating in June 2019. The site allowed users to engage in online communications with other users, either within forums that were openly accessible to any user of the site, within forums only accessible to particular users, or in one-to-one private message chats between two users.

16. The registration page required prospective users to create a user name and password, to identify the user's language and time zone, and to enter a generated confirmation code. By clicking on a user's profile, the date a user joined, total posts, most active forum and most active topic were displayed. The rules listed on the site stated:

- i) Hosts that require javascript, Flash, Java and other plugins to function entirely, may not be linked here.
- ii) It is forbidden to reveal your personal information or personal information of another.
- iii) It is forbidden to sell or trade anything (this includes any offer or request, to send material by Private Messages).
- iv) Constructive criticism is accepted, negative criticism without a solution, are not.
- v) Any language is allowed, but unless writing in the appropriate language sub-forum, an English translation should be provided.

17. Upon entry to the site, users were presented with "announcement," "rules," "allowed hosts," "videos," and "photos" sections. The "video" and "photo" sections offered links to topics such as "hardcore," "adolescents," "toddlers," "spycam," "soft hurtcore." There were descriptions of each topic such as the description for "toddlers" was "0-4 years", "Fetish" was "cross-dressing, diaper, scat, zoo, etc," and "soft hurtcore" was "fighting, wrestling, bondage, spanking, etc."

18. Child pornography images and videos were trafficked through this chat site via the posting of web links within forum messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos are stored, in order to download these image and videos. Entry to the site was obtained through free registration. Users were provided with numerous links to image hosts where users could upload their digital images. For instance, on [REDACTED] the user [REDACTED] posted a hyperlink of a .jpeg file named "http://il2.pixs.ru/storage/5/7/0/ToddlerBoy\_5527045\_31141570.jpg", which depicted an image of a prepubescent male toddler, naked from the waist down with his legs spread apart, having a bottle inserted into his anus. FBI Special Agents accessed and downloaded

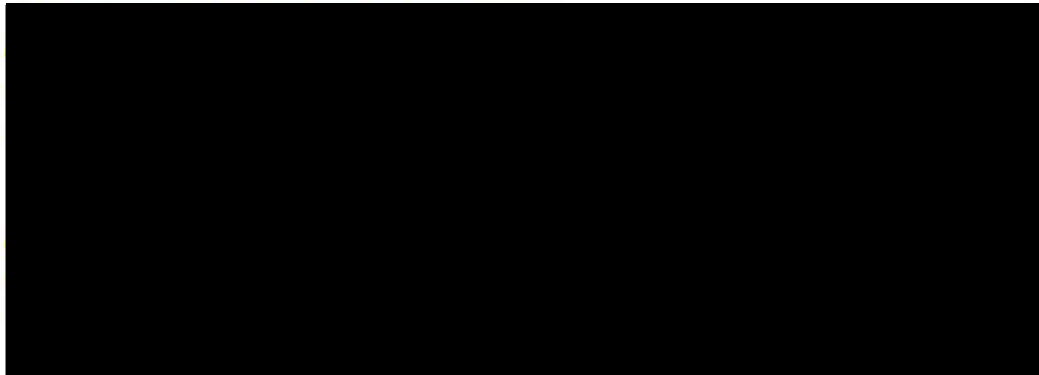


child pornography and child erotica files via links that were posted on the TARGET WEBSITE, in an undercover capacity, from computers located in the Eastern District of Virginia.

*Id.* at ¶¶ 15-18.

**Evidence that Subject IP Address Accessed Target Website**

In a section of the affidavit titled "Evidence Related to Identification of Target that Accessed TARGET WEBSITE," SA Fallon indicates that he is "aware that U.S. as well as foreign law enforcement agencies investigate anonymous offenders engaging in online child sexual exploitation via Tor hidden service websites such as the site(s) described herein." *Id.* at ¶ 19. SA Fallon indicates that because the websites are globally accessible, the websites and their users may be located anywhere in the world. *Id.* He further indicates that "[d]ue to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located. Accordingly, when a law enforcement agency obtains evidence that such a website or website user may be located in another country, it is common practice for that law enforcement agency to share information with a law enforcement agency in the country where the site is located or the offender appears to reside, in accordance with each country's laws." *Id.* According to SA Fallon:





*Id.* at ¶¶ 20-21 (italics typeface in original).

SA Fallon asserts that he is aware through his training, experience, and consultation with other U.S. law enforcement agents that “tips provided by FLA regarding IP addresses that FLA advised were associated with access to Tor network child exploitation-related web and chat sites have: (1) led to the identification and arrest of a U.S.-based child pornography producer and hands-on offender, and the identification and rescue of multiple U.S. children subject to that offender's ongoing abuse; (2) led to the seizure of evidence of child pornography trafficking and possession; and (3) been determined through further investigation to be related to targets that U.S. law enforcement investigation had independently determined were associated with child pornography trafficking and possession.” *Id.* at ¶ 22.

SA Fallon indicates that the Target Website could not generally be accessed through the traditional internet, and that “[o]nly a user who had installed the appropriate Tor software on the user's computer could access ‘TARGET WEBSITE.’” *Id.* at ¶ 23. He further indicates that “[e]ven after connecting to the Tor network, however, a user would

have to find the 16-or-56 character web address of 'TARGET WEBSITE' in order to access it." *Id.* He indicates that hidden service websites on the Tor Network are not "indexed" by search engines, such as Google, "to anywhere near the same degree as websites that operate on the open Internet. Accordingly, it is much more difficult to perform a Google-type search of hidden service websites than it is to search open Internet websites for particular content of interest." *Id.* He indicates that users "interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content." *Id.* He indicates that "[t]hose directory sites also operate via the Tor network. Users utilize those directory sites to identify new web forums, chat sites, image galleries and file hosts pertaining to the sexual exploitation of children. Such directory sites often identify whether particular sites are then operating, whether child pornography imagery may be found there, and even what types of child pornography are accessible (*i.e.*, boys, girls, or "hurtcore"). They also contain clickable hyperlinks to access those sites." *Id.* He indicates that "[a]s with other hidden service websites, a user must find the 16-or-56 character web address for a directory site in order to access it." *Id.* SA Fallon indicates that while it operated, "the web address for the website described herein was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children." *Id.*

Based on consultation with other FBI agents, SA Fallon described user data "related to one prominent Tor network based child pornography website," "Playpen." *Id.* at



¶ 24. According to SA Fallon, Playpen was a Tor network-based hidden service "dedicated to the advertisement and distribution of child pornography that operated from August 2014 until March 2015" that the FBI seized and operated for two weeks in February and March of 2015 using a court authorized investigative technique to identify IP addresses and other information associated with site users. *Id.* SA Fallon indicates that "[s]imilar to TARGET WEBSITE, Playpen was a highly categorized web forum with hundreds of thousands of users. It allowed users to post and download messages pertaining to child exploitation within forum categories indexed by the age and gender of child victims and the type of sexual activity involved." *Id.* He further indicates that "FBI review of site data seized from the Playpen website during the operation determined that of over 400,000 total user accounts observed on the Playpen website during its existence, less than 0.02 percent (that is, less than two hundredths of one percent) of user accounts registered an account on the website, accessed a message thread on the website, and then never returned to the site and logged into the same account." *Id.*

SA Fallon then asserts:

25. Based on my training and experience, because accessing TARGET WEBSITE required numerous affirmative steps by the user - to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor - it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.

26. Accordingly, I submit that there is probable cause to believe that, for all of the reasons described herein, any user who accessed TARGET WEBSITE has, at a minimum, knowingly accessed the TARGET WEBSITE with intent to view child pornography, or attempted to do so.

*Id.* at ¶¶ 25-26.

SA Fallon's affidavit indicates that through an administrative subpoena to Charter Communications it was learned that Defendant was the account holder/subscriber for IP address 69.206.190.157 (*i.e.*, the IP address identified by the FLA as accessing the Target Website on April 22, 2019), had a subscriber address at the Subject Premises in New Paltz, New York, and had an Email address of "delaneyj3@hawkmil.newpaltz.edu." *Id.* at ¶¶ 27-28. FBI agents also learned from other sources that the defendant was a graduate student at the State University of New York at New Paltz ("SUNY New Paltz"), lived at the Subject Premises, was believed to have studied Early Childhood Education, and had submitted an application for employment with the New York State Department of Education on March 24, 2016. *See id.* at ¶¶ 29-34.

#### **Child Pornography, Computers, and the Internet**

SA Fallon asserts that based on his training and experience in the investigation of computer-related crimes, he knows, *inter alia*, that computers and digital technology are the primary way in which individuals interested in child pornography interact with each other, and that computers basically serve the functions of production, communication, distribution, and storage of child pornography, *id.* at ¶ 35(a); that child pornography can "be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone," *id.* at ¶ 35(c); that computers and electronic storage media of various types can store images or videos of child pornography, *id.* at ¶ 35(d); that even in cases where online storage is used, "evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases," *id.* at ¶ 35(f); and that:

communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one's favorite websites in, for example, "bookmarked" files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

*Id.* at ¶ 35(h).

**Characteristics Common to Individuals Who Produce, Advertise,  
Transport, Distribute, Receive, Possess, And/or Access with Intent  
To View Child Pornography**

Based on SA Fallon's previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom he has had discussions, he sets forth certain characteristics common to individuals who access online child sexual abuse and exploitation material via a website. *Id.* at ¶¶ 36(a)-(h). This includes that "[s]uch individuals may collect sexually explicit or suggestive materials in a variety of media" and use these materials for a variety of reasons including "for their own sexual arousal and gratification, . . . to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts," *id.* at ¶ 36(b), that "[s]uch individuals almost always possess and maintain their hard copies of child pornographic material . . . in the privacy and security of their home or some other secure location," and "typically retain their pictures, films, video tapes, photographs, magazines, negatives, correspondence, mailing lists, books, tape recordings and child erotica for many years," *id.* at ¶ 36(c), and that "such individuals often



maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area,” that “[t]hese child pornography images are often maintained for several years and are kept close by . . . to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.” *Id.* at ¶ 36(d). SA Fallon asserts that even if child pornography is downloaded on a computer or digital device and then deleted, forensic tools exist to discover evidence of the crime for extended periods of time even after the individual “deleted” it. *Id.* at ¶ 36(e). SA Fallon also asserts that “[s]uch individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses (including email addresses), and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.” *Id.* at ¶ 36(f). SA Fallon’s affidavit indicates that he believes “that an internet user residing at the SUBJECT PREMISES likely displays characteristics common to individuals who access online child sexual abuse and exploitation material via a website. For example, the target of investigation obtained and used Tor network software, found the web address for TARGET WEBSITE, and accessed online child sexual abuse and exploitation material via TARGET WEBSITE.” *Id.* at ¶ 37.

#### **Specifics of Search and Seizure of Computer Systems**

SA Fallon indicates that, through the warrant, law enforcement “seeks permission

to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other storage media." *Id.* at ¶ 38. SA Fallon maintains "if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records referenced above will be stored on that computer or storage medium" *id.* at 39, because:

- a. Deleted files, or remnants of deleted files, may reside in free space or slack space--that is, in space on the storage medium that is not currently being used by an active file--for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.
- b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.
- c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.
- d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

*Id.* at ¶¶ 39(a)-(d).

SA Fallon indicates that the warrant application "seeks permission to locate



not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. *Id.* at ¶ 40. He indicates that

there is probable cause to believe that this forensic electronic evidence will be on any storage medium in the SUBJECT PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpatng or exculpatng the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the



crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for

evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

*Id.* at ¶¶ 40(a)-(f).

SA Fallon indicates that based upon his training and experience and information relayed to him by agents and others involved in the forensic examination of computers, he knows that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and online or off site storage servers maintained by corporations, including but not limited to "cloud" storage. *Id.* at ¶ 41. He also indicates that he knows that during the search of a premises, it is not always possible to search computer equipment and storage devices for data because, *inter alia*, searching computer systems is a highly technical process that requires specific expertise and specialized equipment which may not be possible to employ at the search site while maintaining the integrity of the evidence and recovering "hidden," erased, compressed, encrypted, or password-protected data, *id.* at ¶¶ 41(a)-(b); the large volume of data stored on many computer systems and storage devices makes it impracticable to search for data during the execution of the physical search of the premises, *id.* at ¶ 41(c); and computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading



filenames and extensions, *id.* at ¶ 41(d). SA Fallon also indicates that based upon his training and experience and information relayed to him by agents and others involved in the forensic examination of computers, he knows that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. *Id.* at ¶ 42. Based on the foregoing, SA Fallon sought a warrant that would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant, and that would authorize a later review of the media or information consistent with the warrant. *Id.* at ¶ 43.

**b. Execution of the Search Warrant**

Law enforcement officers executed the search warrant at Defendant's residence in New Paltz, New York on December 12, 2019. Upon execution, law enforcement seized electronic devices, including a Dell Laptop, KESU hard drive and Cruzer thumb drive from the Defendant's bedroom. See Def. Ex. G. An initial forensic preview of the Dell Laptop and KESU hard drive revealed videos and images of minor boys engaged in sexually explicit conduct. See Crim. Compl. Aff., Dkt. No. 1, ¶¶ 7-8. Within the KESU hard drive, the videos were in a folder titled "Tor Browser." *Id.*

During the execution of the search warrant, after being told that he was not under arrest and did not have to have to talk to SA Fallon, see Gov. Ex. 1 at 2:34 (Delaney Residence Interview, filed under seal), Defendant admitted that he owned and used the Dell Laptop and provided the password for the laptop. See *id.* at 9:24; see also Dkt. No. 1, ¶ 9. Defendant also admitted that he downloaded child pornography from a website and



saved the videos of child pornography to his Dell Laptop. See Gov. Ex. 1 at 10:19, 13:50. The government contends that the defendant voluntarily went with investigators from his residence to the New York State Police Highland Station. He was again told that he was not in custody and was not handcuffed. *Id.* at 11:40. Once at the station, the Defendant confirmed that he went with the officers voluntarily to the station and confirmed what he told SA Fallon at his residence. See Gov. Ex. 2 at 2:40 (Delaney Highland Station Interview, filed under seal). SA Fallon read the defendant his *Miranda* rights during that conversation and the defendant signed a waiver of rights form and agreed to continue speaking with investigators. See Gov. Ex. 2 at 4:45-6:00; Gov. Ex. 3 (Waiver of Rights Form, filed under seal). The defendant described child pornography videos that he viewed and downloaded. See Gov. Ex. 2 at 7:10-11:00, 13:20-14:30. The defendant also participated in a post-polygraph, post-*Miranda*, recorded interview in which he made additional admissions and provided a handwritten statement. See Def. Ex. I (FBI FD-302, filed under seal); see generally, Gov. Ex. 4 (Delaney Post-Polygraph Interview, filed under seal).

### **c. Procedural Background**

On December 12, 2019, Defendant was arrested and charged by way of felony complaint with possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). See Dkt. No. 1. Defendant was initially arraigned and held in custody pending a detention hearing on December 13, 2019. At the December 13, 2019 detention hearing, Judge Stewart released the defendant to the supervision of U.S. Probation under terms of house arrest. See Dkt. No. 4. On October 29, 2020, Defendant was indicted by a Grand Jury in

the Northern District of New York on the four (4) counts indicated above.

### III. LEGAL FRAMEWORK

#### a. Probable Cause

The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. Probable cause is “a fluid concept—turning on the assessment of probabilities in particular factual contexts—not readily, or even usefully, reduced to a neat set of legal rules.” *Illinois v. Gates*, 462 U.S. 213, 232 (1983). “The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the ‘veracity’ and ‘basis of knowledge’ of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Id.* at 238. “[O]nly the probability, and not the prima facie showing, of criminal activity is the standard of probable cause.” *Id.* at 235 (internal quotation marks and citation omitted); *see also United States v. Martin*, 426 F.3d 68, 74 (2d Cir. 2005).<sup>4</sup>

---

<sup>4</sup>In *Martin*, the Second Circuit wrote:

The Supreme Court has held that probable cause does *not* require a “prima facie showing”:

Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence, useful in formal trials, have no place in the magistrate’s decision. While an effort to fix some general, numerically precise degree of certainty corresponding to “probable cause” may not be helpful, it is clear that “only the probability, and not a prima facie showing, of criminal activity is the standard of probable cause.”

426 F.3d at 74 (quoting *Gates*, 462 U.S. at 235, in turn quoting *Spinelli v. United States*, 393 U.S. 410, 419 (1969))(emphasis in *Martin*).

“In assessing the proof of probable cause, the government's affidavit in support of the search warrant must be read as a whole, and construed realistically.” *United States v. Salameh*, 152 F.3d 88, 113 (2d Cir. 1998)(citing *Gates*, 462 U.S. at 230–31).

“After-the-fact scrutiny by courts of the sufficiency of an affidavit should not take the form of *de novo* review. A magistrate's determination of probable cause should be paid great deference by reviewing courts.” *Gates*, 462 U.S. at 236 (internal citations and quotation marks omitted). “A grudging or negative attitude by reviewing courts toward warrants, is inconsistent with the Fourth Amendment's strong preference for searches conducted pursuant to a warrant [, and] courts should not invalidate warrants by interpreting affidavits in a hypertechnical, rather than a commonsense, manner.” *Id.* (internal citations and quotation marks omitted).

“Due to this subjective standard, a reviewing court generally accords ‘substantial deference to the finding of an issuing judicial officer that probable cause exists,’ limiting [the court’s] inquiry to whether the officer ‘had a substantial basis’ for his determination.” *United States v. Raymonda*, 780 F.3d 105, 113 (2d Cir. 2015) (quoting *United States v. Wagner*, 989 F.2d 69, 72 (2d Cir.1993)); see *Salameh*, 152 F.3d at 113 (A reviewing court’s “duty is ‘simply to ensure that the magistrate had a ‘substantial basis for ... conclud[ing]’ that probable cause existed.”)(quoting *Gates*, 462 U.S. at 238–39 (citation omitted; alterations in original)). Given the deference accorded a judge’s determination that probable cause exists, courts “resolve any doubt about the existence of probable cause in favor of upholding the warrant.” *Salameh*, 152 F.3d at 113 (citing *United States v. Jakobetz*, 955 F.2d 786, 803 (2d Cir. 1992)). “Even applying this standard, however, [a



court] may conclude that a warrant is invalid where the magistrate's 'probable-cause determination reflect[s] an improper analysis of the totality of circumstances.'" *Raymonda*, 780 F.3d at 113 (quoting *United States v. Falso*, 844 F.3d 110, 117 (2d. Cir. 2008))(internal quotation marks omitted).

#### **b. Staleness**

In addition, a court "may conclude that a warrant lacks probable cause where the evidence supporting it is not 'sufficiently close in time to the issuance of the warrant' that 'probable cause can be said to exist *as of the time of the search*'—that is, where the facts supporting criminal activity have grown stale by the time that the warrant issues." *Id.* at 114 (quoting *Wagner*, 989 F.2d at 75)(emphasis added in *Raymonda*). There is no bright-line rule for staleness, and instead staleness must be evaluated on the basis of the facts of each case. *Id.* (citing *Walczyk v. Rio*, 496 F.3d 139, 162 (2d Cir. 2007) and *United States v. Martino*, 664 F.2d 860, 867 (2d Cir. 1981)). "The two critical factors in determining staleness are the age of the facts alleged and the 'nature of the conduct alleged to have violated the law.'" *Id.* (quoting *United States v. Ortiz*, 143 F.3d 728, 732 (2d Cir.1998)(internal quotation marks omitted)). Where the supporting affidavit "establishes a pattern of continuing criminal activity,' such that 'there is reason to believe that the cited activity was probably not a one-time occurrence,' the passage of time between the last alleged event and the warrant application is less significant." *Id.* (quoting *Wagner*, 989 F.2d at 75)

The Second Circuit has "recognized that the determination of staleness in investigations involving child pornography is unique." *Id.* (citing *United States v. Irving*, 452

F.3d 110, 125 (2d Cir. 2006)). This is “[b]ecause it is well known that images of child pornography are likely to be hoarded by persons interested in those materials in the privacy of their homes.” *Id.* (internal quotation marks and citation omitted). “[E]vidence that such persons possessed child pornography in the past supports a reasonable inference that they retain those images—or have obtained new ones—in the present.” *Id.* (citations omitted). “Crucially, however, the value of that inference in any given case depends on the preliminary finding that the suspect is a person ‘interested in’ images of child pornography.” *Id.* “The ‘alleged ‘proclivities’ of collectors of child pornography,’ that is, ‘are only relevant if there is probable cause to believe that [a given defendant] is such a collector.’” *Id.* (quoting *United States v. Coreas*, 419 F.3d 151, 156 (2d Cir. 2005))(emphasis added in *Raymonda*). “Federal courts including [the Second Circuit] have historically inferred that a suspect is a ‘collector’ of child pornography, likely to hoard illicit images, based on a number of factors.” *Id.* These include a suspect’s admission or other evidence identifying him as a “pedophile,” information indicating that the suspect paid for access to child pornography, or where the suspect had an extended history of possessing or receiving pornographic images. *Id.* (citations omitted).

In certain circumstances, courts have even inferred that a suspect was a hoarder of child pornography on the basis of a single incident of possession or receipt. They have done so where, for example, the suspect’s access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files. *See, e.g., [United States v. Vosburgh*, 602 F.3d 512, 528 (3d Cir. 2010)] (finding no staleness where suspect could not have accessed images “with a simple click of the mouse,” but had to enter decoded URL address and decrypt ensuing download, *id.* at 517); *United States v. Hay*, 231 F.3d 630, 634, 636 (9th Cir. 2000) (finding no staleness where suspect received 19 files within seven minutes through file transfer protocol). Or they have done so where the defendant, having accessed a single file of child pornography, subsequently

redistributed that file to other users. *See, e.g., United States v. Seiver*, 692 F.3d 774, 775–77 (7th Cir. 2012) (finding no staleness where suspect downloaded single video and subsequently uploaded still images from video to Internet).

In all of these cases, the inference that the suspect was a collector of child pornography did not proceed merely from evidence of his access to child pornography at a single time in the past. Rather, it proceeded from circumstances suggesting that he had accessed those images willfully and deliberately, actively seeking them out to satisfy a preexisting predilection. Such circumstances tend to negate the possibility that a suspect's brush with child pornography was a purely negligent or inadvertent encounter, the residue of which was long ago expunged. They suggest that the suspect accessed those images because he was specifically interested in child pornography, and thus—as is common among persons interested in child pornography—likely hoarded the images he found.

*Id.* at 115.

### **c. Good-Faith Exception to the Exclusionary Rule**

To effectuate the rights protected by the Fourth Amendment, “courts have created an exclusionary rule ‘that, when applicable, forbids the use of improperly obtained evidence at trial.’” *United States v. Eldred*, 933 F.3d 110, 118 (2d Cir. 2019)(quoting *Herring v. United States*, 555 U.S. 135, 139 (2009)). However, a determination that a Fourth Amendment violation occurred “does not automatically require the suppression of all physical evidence seized or statements derived from that illegal search.” *United States v. Bershchansky*, 788 F.3d 102, 112 (2d Cir. 2015). As the Second Circuit has stated, “[e]ven when a search warrant is constitutionally defective, we bear in mind that ‘[s]uppression of evidence ... has always been [a] last resort, not [a] first impulse.’” *United States v. Purcell*, 967 F.3d 159, 179 (2d Cir. 2020)(quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)). “To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such



deterrence is worth the price paid by the justice system.” *Herring*, 555 U.S. at 144.

“[S]uppression of evidence obtained pursuant to a warrant should be ordered only on a case-by-case basis and only in those unusual cases in which exclusion will further the purposes of the exclusionary rule.” *United States v. Leon*, 468 U.S. 897, 918 (1984); see *Herring*, 555 U.S. at 141 (“[T]he exclusionary rule is not an individual right and applies only where it results in appreciable deterrence.”)(internal quotation marks and brackets omitted).

In *Leon*, the Supreme Court set out an exception to the exclusionary rule for a search conducted in “reasonable, good-faith reliance on a search warrant that is subsequently held to be defective.” *Leon*, 468 U.S. at 905. “[E]vidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion” and will not be suppressed. *Leon*, 468 U.S. at 922. In determining whether to apply the good faith exception, courts examine “whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances.” *United States v. Rosa*, 626 F.3d 56, 64 (2d. Cir. 2010) (internal quotations and citations omitted). However, the so-called good faith exception to the exclusionary rule does not apply “(1) where the issuing magistrate has been knowingly misled; (2) where the issuing magistrate wholly abandoned his or her judicial role; (3) where the application is so lacking in indicia of probable cause as to render reliance upon it unreasonable; and (4) where the warrant is so facially deficient that reliance upon it is unreasonable.” *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011)(citing *Leon*, 468 U.S. at 923).

#### IV. DISCUSSION

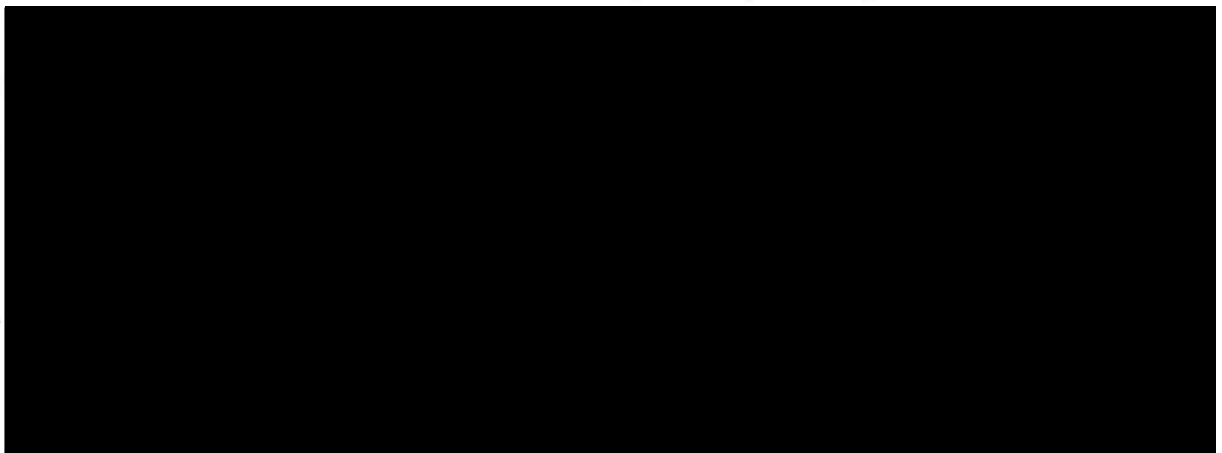
##### a. Probable Cause

As indicated above, Defendant primarily presents two arguments challenging the probable cause finding. He contends that (1) there was insufficient evidence demonstrating a fair probability that Defendant's IP address accessed the Target Website, and (2) the facts underlying the warrant application are independently deficient and stale. After considering the parties' arguments and precedential authority, the probable cause determination is a close call.

##### 1. Whether Someone Using Defendant's IP address Accessed the Target Website

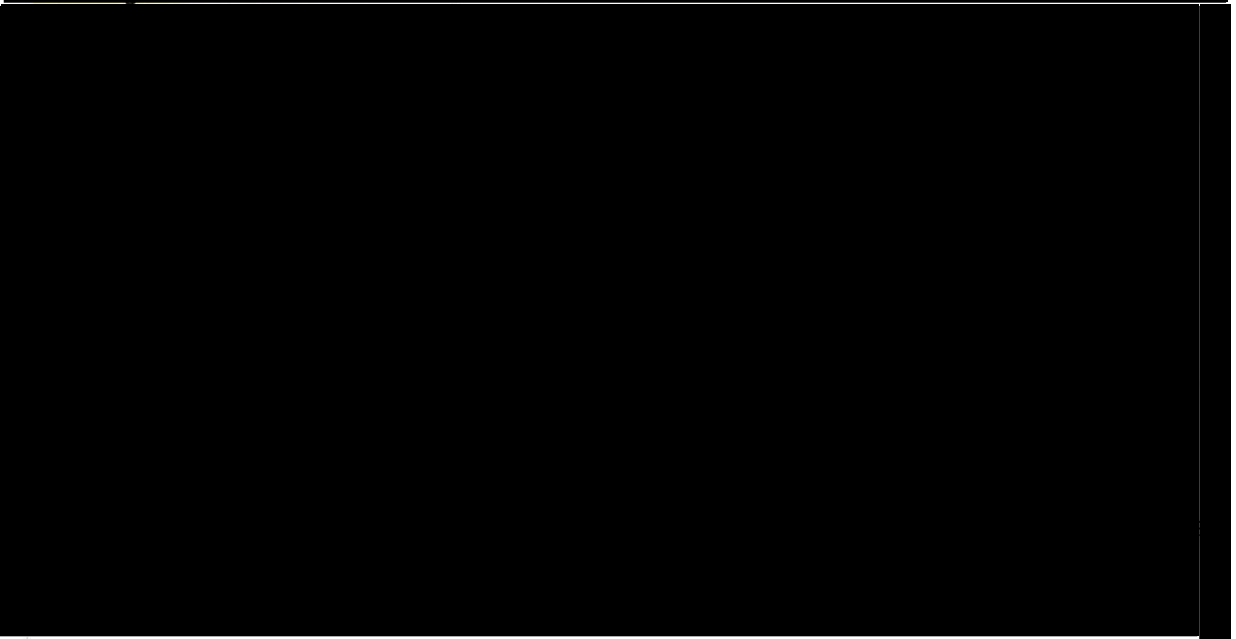
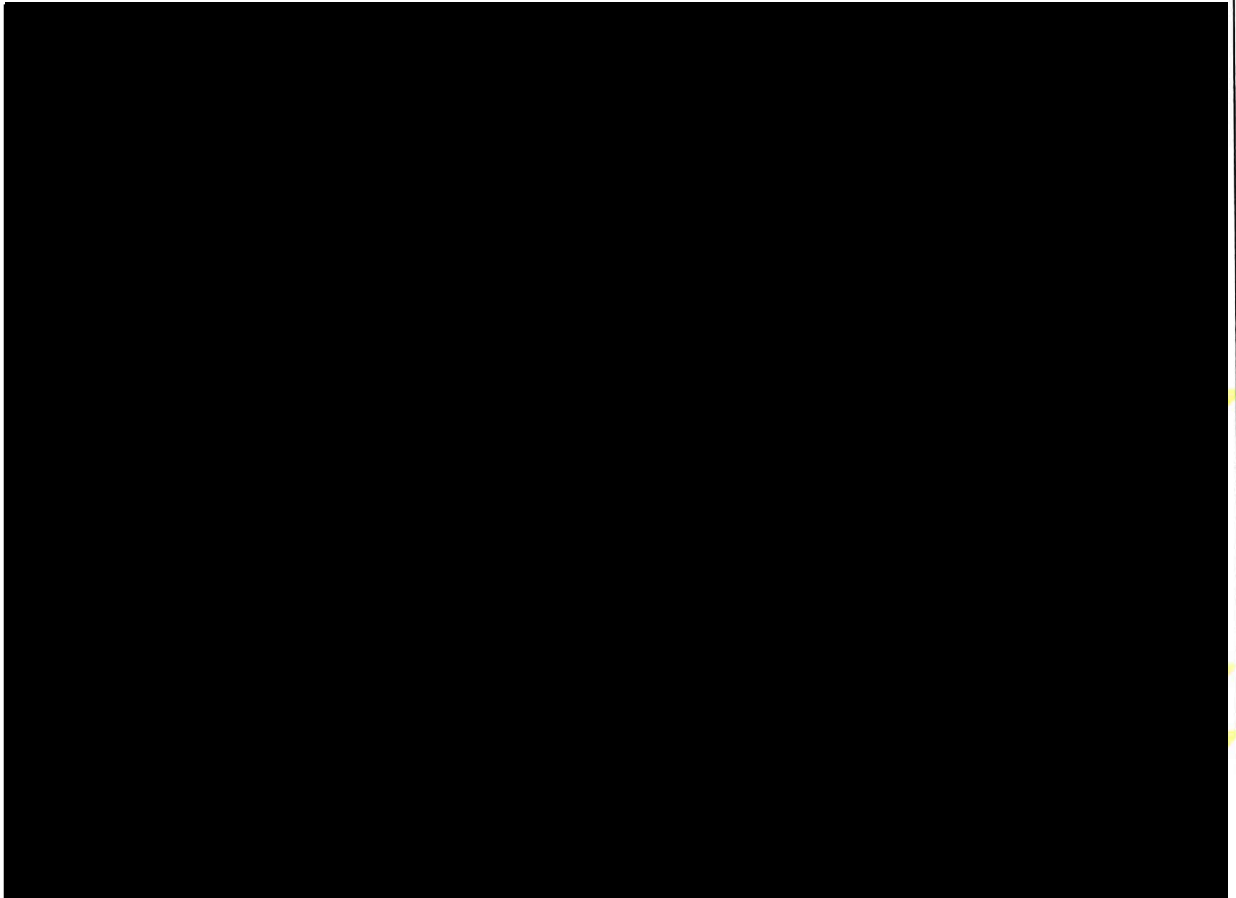
Defendant presents a strong argument that SA Fallon's affidavit fails to provide a substantial basis demonstrating a fair probability that someone using Defendant's IP address accessed the Target Website. Defendant points to SA Fallon's several statements indicating that it can be difficult if not impossible to determine whether an IP address accessed the Target Website using traditional IP address-based identification techniques, or rather whether the subject IP address served as a relay or exit node in the Tor network in which the Target Website operated. In this regard, SA Fallon asserts the Target Website could only be accessed using the Tor network, which is a network of linked computers that masks a user's identity, Dkt. No. 46-6 ¶¶ 8-9, 23; that the Tor network was designed specifically to facilitate anonymous communications over the Internet, *id.* at ¶ 8; that "[t]he Tor network attempts to do this by routing Tor user communications through a globally distributed network of intermediary computers, or relays, along a randomly assigned path known as a 'circuit,'" *id.*; that "the content of a Tor

user's communications are encrypted while the communication passes through the Tor network" which "can prevent the operator of a Tor node from observing the content (but not the routing information) of other Tor users' communications," *id.* ¶ 11; that "due to the anonymity provided by the Tor network, it can be difficult or impossible to determine, at the beginning of an investigation, where in the world a particular website or user is located," *id.* at ¶ 19; that "when a Tor user accesses an Internet website, only the IP address of the last relay computer (the "exit node") as opposed to the Tor user's actual IP address, appears on the website's IP log," *id.* at ¶ 11; and that "[b]ecause of the way the Tor network routes communications through the relay computers, traditional IP address-based identification techniques are not effective." *Id.* at ¶ 8.<sup>5</sup> Based only on SA Fallon's representations as to how the Tor network was structured and the inability of traditional IP address-based identification techniques to identify IP addresses other than at the exit node, it is unclear whether the subject IP address was used by the actual Target User to access the Target Website, or if it was the exit node or a Tor relay used by the Target User.



<sup>5</sup>Defendant notes that "[a]lthough not included in the warrant application, SA Fallon's understanding of the TOR network is corroborated in the investigatory lead information sent to the FBI's Albany Division about this case, which stated that because of the Tor network's structure, '[c]urrently, there is no practical method to trace a user's actual IP address back through those Tor relay computers.'" Dkt. No. 46-2 at 5, n. 1 (quoting Def. Ex. D, Dkt. 46-5 (sealed) at pg. 3).





It is well settled that an affidavit to a search warrant that relies on hearsay “is not to be deemed insufficient on that score, so long as a substantial basis for crediting that hearsay is presented.” *Gates*, 462 U.S. at 241- 42 (interior quotation marks and citation omitted). Defendant argues that the FBI should have sought a pen register/trap and trace pony (“PRTT”) to determine whether Tor network traffic was coming from Defendant’s residence, as suggested by the FBI’s referral to the Albany Field Office. See Def. Ex. D, Dkt. 46-5 (sealed). This apparently was not done and there is no explanation by the Government why it was not.

The failure to seek a PRTT, which might have provided additional corroboration for the FLA’s determination,<sup>6</sup> gives the Court some pause in determining whether probable cause existed. See *Falso*, 544 F.3d at 124, n. 20.<sup>7</sup> However, the absence of such evidence is not fatal to whether a substantial basis supported the conclusion that the subject IP address accessed the Target Website. According to SA Fallon’s affidavit, the hearsay tip was from a known law enforcement agency with which U.S. law enforcement agencies had a long history of cooperation in fighting child abuse crimes, and the FLA had provided reliable information in the past in similar criminal prosecutions. Under these circumstances, there was a sufficient basis for Judge Stewart to deem reliable the FLA’s determination that the subject IP address accessed the Target Website. See, e.g., *United*

---

<sup>6</sup>The Court notes that the FBI referral to the Albany Field Office, which was not referenced in SA Fallon’s affidavit, was made on November 18, 2019, whereas SA Fallon’s affidavit indicates that the Target Website ceased operation in June 2019. It may have well been that FBI agents in Albany thought a PRTT application seeking communication with the Target Website would have been futile in November 2019.

<sup>7</sup>(“As we admonished in *Coreas*, the “[g]overnment could easily have obtained more information” about *Falso*. See *Coreas*, 419 F.3d at 158. Among other things, it could have monitored the traffic of the cpfreedom.com website and ascertained whether *Falso* (and others) actually downloaded pornography from the site. See *id.*”)


*States v. Ventresca*, 380 U.S. 102, 111 (1965)(“Observations of fellow officers of the Government engaged in a common investigation are plainly a reliable basis for a warrant applied for by one of their number.”)(footnote omitted); *United States v. Mathurin*, 561 F.3d 170, 176 (3d Cir. 2009)(“We need not undertake the established legal methods for testing the reliability of this tip because a tip from one federal law enforcement agency to another implies a degree of expertise and a shared purpose in stopping illegal activity, because the agency's identity is known.”); *United States v. Benoit*, 730 F.3d 280, 285 (3d Cir. 2013)(Extending the rationale of *Mathurin* to foreign law enforcement authorities and finding that it was reasonable for the U.S. Coast Guard to rely on information received from Grenadian law enforcement authorities, given that the source of the tip “was not only known to the DEA, but was also a repeat player in the United States' efforts at drug trafficking prevention,” and finding that “[t]he working relationship between Grenada and the United States bolsters the credibility of the information, since the Grenadian authorities' ‘reputation can be assessed,’ and they ‘can be held responsible if [their] allegations turn out to be fabricated.’”)(quoting *Florida v. J.L.*, 529 U.S. 266, 270 (2000)); *United States v. McKenzie*, No. 1:14 CR 169 (MAD), 2015 WL 13840885, at \*9 (N.D.N.Y. Nov. 4, 2015)(“Government investigatory agents are entitled to a ‘presumption of credibility’ when a court evaluates their hearsay information in an affidavit.”)(quoting and citing *United States v. Morill*, 490 F. Supp. 477, 478 (S.D.N.Y. 1980) (finding probable cause in an affidavit based in part on hearsay information provided by federal and local law enforcement agents), and citing *Ventresca*, 380 U.S. at 111; *Velardi v. Walsh*, 40 F.3d 569, 574 (2d Cir. 1994)). Moreover, at least one District Court addressed a similar



circumstance where a Magistrate Judge issued a search warrant based on a tip from an FLA that a defendant had accessed a child pornography website in the Tor network. See *United States v. Sanders*, 1:20-cr-00143 (TSE), Dkt. No. 122, at 9 (Oct. 29, 2020, E.D. Va.). The District Court in *Sanders* found that because the FLA had a “history of providing reliable tips to the FBI” and was “a respected foreign law enforcement agency,” “it was reasonable for the Magistrate Judge to rely on the FLA Tip without further corroboration by the FBI.” *Id.* SA Fallon’s affidavit indicating that the FLA providing the tip has a long history of providing reliable information and is a known and respected foreign law enforcement agency decreases the need for corroboration.

Further, according to SA Fallon, the FLA obtained its information through an independent investigation lawfully authorized in the FLA’s country pursuant to its national laws. While SA Fallon’s affidavit does not explain the specific technique that the FLA used to identify the subject IP address as having accessed the Target Website, that does not mean that such an identification is impossible even in the Tor network where identification of IP addresses other than in the exit node is extremely difficult or impossible using traditional identification techniques. Indeed, as FA Fallon’s affidavit indicates, the FBI previously seized and briefly operated the Tor network Playpen website using a court authorized investigative technique to successfully identify IP addresses and other information associated with site users. Dkt. 46-6 ¶ 24. The investigative technique used by the FBI to identify the IP addresses of Playpen users has been recognized by several courts including the Second Circuit. See, e.g., *United States v. Eldred*, 933 F.3d 110, 111

(2d Cir. 2019);<sup>8</sup> *United States v. Wheeler*, No. 1:15-CR- 00390 (MHC/JFK), 2017 WL 9472982, at \*3-4 (N.D. Ga. June 12, 2017), *report and recommendation adopted*, 2017 WL 3589564 (N.D. Ga. Aug. 21, 2017).<sup>9</sup>



upon all of this, the Court finds that there was a substantial basis to conclude that the subject IP address accessed online child sexual abuse and exploitation material via the Target Website on April 22, 2019.

**2. Whether the Facts Underlying the Warrant Application Are Independently Deficient and Stale**

Defendant argues that even if the evidence demonstrates that the subject IP

---

<sup>8</sup>("This case arises from one of the many prosecutions following the investigation by the Federal Bureau of Investigation ('FBI') into Playpen, a child pornography site located on the dark web. The FBI infiltrated the website and discovered the identities of many registered users by deploying a search program, the Network Investigative Technique ('NIT'), which allowed the FBI to circumvent the anonymizing features of the dark web and collect computer-related identifying information, including internet protocol ('IP') addresses, from the computers of these Playpen users.")

<sup>9</sup>(After the FBI operated a server assuming administrative control of Playpen, a website in the Tor network, the FBI utilized a Network Investigative Technique to identify users and IP addresses that accessed the Playpen website)

address accessed the Target Website, the evidence at most demonstrates a single alleged visit of an unknown duration seven and a half months before the warrant was sought. Defendant maintains that suppression is required because the facts underlying the warrant application are independently deficient and stale.

**A. Independently Deficient**

Defendant notes that while the application states that the Target Website's users needed to register for an account to access the vast majority of the contraband material, SA Fallon provided no evidence that Defendant or a user using the subject IP address was a registered user or logged into a preexisting account on April 22, 2019 or at any other time. Defendant also points out that although SA Fallon indicates that detailed data about individual users and their activity on the Target Site, like the "date a user joined, total posts, most active forum and most active topic," is available simply by clicking on a user's name, no such information related to these data points is provided in the application regarding the targeted user or the Defendant.

In addition, Defendant stresses that there is no evidence that the targeted user or the Defendant saved any illicit images or accessed or viewed the specific contraband images described in ¶ 18 of the application as being trafficked through the site. Furthermore, Defendant maintains that there is no indication that the Government attempted to follow up with the FLA regarding these issues.

Defendant acknowledges that the application states that "users were able to view some material without creating an account," but maintains that "some material" is never described or defined. Similarly, Defendant maintains that while the application incorporated the FLA's statement that the subject IP address "accessed online child



sexual abuse material via the Target Site,” “online child sexual abuse material” is not defined by the FLA or SA Fallon. Defendant argues that while SA Fallon defines terms such as “child pornography,” “child erotica,” “sexually explicit conduct,” and “visual depiction,” he never defines or identifies “online child sexual abuse material” as child pornography, child erotica, sexually explicit conduct or any kind of contraband. Defendant also points out that there is no information provided about what the phrase “online child sexual abuse material” means under the FLA’s country’s laws, and asserts that the “online sexual abuse material” described by the FLA could merely be text regarding the Target Site and available content as opposed to actual contraband images or videos. Defendant argues that the failure to particularize and define the term “online sexual abuse material” means that the Court “cannot conclude or infer that the material the FLA referred to was actually contraband, when broad terms like ‘material’ used by a foreign entity could mean a host of things that is not indicative of criminal conduct.”

When read within the totality of the allegations in SA Fallon’s affidavit and applying a common-sense interpretation of these allegations, Defendant’s arguments are insufficient to defeat the probable cause finding. Although there is no evidence or allegation that Defendant or anyone using the subject IP address was a registered user of the Target Website, the affidavit indicates that, as Defendant acknowledges, users were able to view some material without creating an account. While “some material” is not defined, it is reasonable conclusion in the context of the totality of the allegations that this included viewing child pornography. SA Fallon described in detail the objectives and contents of the Target Website as provided by the FLA and other FBI agents, supplying a substantial basis to conclude that the site’s primary focus was on the advertisement and

distribution of child pornography. See *Martin*, 426 F.3d at 74-76 (describing the website's welcome message and contents that supported the conclusion that the "primary reason for [its] existence, was the trading and collection of child pornography"); *Falso*, 544 F.3d at 121 (noting that the agent's affidavit fell short of providing such a description). For example, SA Fallon explained that upon entry to the Target Website site, users were presented with an announcement, rules, allowed hosts, videos and photos sections, and an indication that the video and photo sections offered links to topics such as "hardcore," "adolescents," and "toddlers," which was described as "0-4 years," Fallon Aff. ¶ 17, providing a reasonable basis to conclude that these videos and photos depicted child pornography. SA Fallon also represented that the FLA determined that the subject IP address "accessed child sexual abuse and exploitation material via a website," and went on to describe the Target Website as having "an explicit focus on the facilitation of sharing child abuse material (images, links and videos), emphasis on indecent material of boys," and that users were able to view some material without creating an account. *Id.* at ¶ 20. Although neither SA Fallon nor the FLA defined the term "child abuse material," given the totality of the allegations in SA Fallon's affidavit, including:

(1) the definition of "child pornography" as being "any visual depiction . . . of sexually explicit conduct" involving a minor, *id.* at ¶ 5(e);

(2) the definition of "sexually explicit conduct" as involving "actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person," *id.* at ¶ 5(p);

(3) the description of the Target Website as "dedicated to the sexual exploitation of minor and/or prepubescent males" where "[t]he advertisement and distribution of child pornography and child erotica were regular occurrences," *id.* at ¶ 15,



(4) where the "video" and "photo" sections of the Target Website offered links to topics such as "hardcore," "adolescents," "toddlers," "spycam," "soft hurtcore," and included descriptions of each topic including the description for "toddlers" as "0-4 years", "Fetish" as "cross-dressing, diaper, scat, zoo, etc," and "soft hurtcore" as "fighting, wresting, bondage, spanking, etc.," *id.* at ¶ 17,

(5) where child pornography images and videos "were trafficked through this chat site via the posting of web links within forum messages," and where links allowed users to navigate to another website such as a file-hosting website where images and/or videos were stored in order to allow downloading of these image and videos,<sup>10</sup>

(6) where one user posted a hyperlink of a .jpeg file which depicted an image of a prepubescent male toddler, naked from the waist down with his legs spread apart, having a bottle inserted into his anus, *id.* at ¶ 18, and from where FBI Special Agents accessed and downloaded child pornography and child erotica files via links that were posted on the Target Website, *id.*,

it was reasonable for Judge Stewart to conclude that the term "online child abuse material" that the FLA indicates that Defendant accessed involved child pornography, that the primary purposes of the Target Website was to provide access to child pornography, and that a user of the subject IP address accessed the Target Website in order to view or attempt to view, and perhaps download, child pornography using a computer.

Furthermore, a series of complicated steps were necessary to access the Target Website, including installing Tor software/browser and finding the 16-56 algorithm-generated characters for the website's web address. See Fallon Aff. ¶ 23. In addition, SA Fallon explained that locating the web address of a hidden service website on

---

<sup>10</sup>It is unclear from SA Fallon's affidavit whether access to the other, file-hosting website required registration in the Target Website, or if this other site had its own free registration. See Fallon Aff. at ¶ 18 ("Child pornography images and videos were trafficked through this chat site via the posting of web links within forum messages. Links allowed a user to navigate to another website, such as a file-hosting website, where images and/or videos are stored, in order to download these image and videos. Entry to the site was obtained through free registration."). For reasons discussed in the text, this uncertainty does not defeat probable cause because the affidavit indicates that an individual could view some material from the Target Website without registration.



Tor is "much more difficult" than performing searches for open Internet websites. *See id.* For this reason, he explained, "[u]sers interested in accessing child exploitation material (or in advertising child exploitation and pornography websites they operate) therefore keep, maintain and use directory sites that advertise the web addresses of hidden services that contain child exploitation related content," and that "[t]hose directory sites also operate via the Tor network." *Id.* He also indicates that "[w]hile it operated, the web address for the [Target Website] was listed on one or more of such directory sites advertising hidden services dedicated to the sexual exploitation of children." *Id.* Given these circumstances, it is a reasonable conclusion that the user of the subject IP address did not stumble upon the target website while searching the Internet, but rather intentionally sought out the website because of the child pornography material that was accessible there. *See id.* ¶ 25.<sup>11</sup> From this, Judge Stewart had a substantial basis to conclude that there was a fair probability that the user of the subject IP address navigated to the Target Website for the purposes of viewing and perhaps downloading child pornography, not that the user inadvertently stumbled upon a child pornography website and closed the website upon learning that it contained child pornography as was potentially the case in *Raymonda*. *See Raymonda*, 780 F.3d at 117 ("Far from suggesting a knowing and intentional search for child pornography, in short, the information in Agent Ouzer's affidavit was at least equally consistent with an innocent user inadvertently

---

<sup>11</sup>("Based on my training and experience, because accessing TARGET WEBSITE required numerous affirmative steps by the user- to include downloading Tor software, accessing the Tor network, finding the web address for TARGET WEBSITE, and then connecting to TARGET WEBSITE via Tor - it is extremely unlikely that any user could simply stumble upon TARGET WEBSITE without understanding its purpose and content.")

stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window.").

The lack of evidence that the Target IP address user actually downloaded any child pornography does not change this conclusion. Sections 2252A(a)(5)(B) and (b)(2) prohibit any person from, *inter alia*, knowingly accessing with the intent to view, or attempting to access with the intent to view, child pornography. Probable cause to believe that Section 2252A has been violated does not require a download. Here, Judge Stewart had sufficient evidence to reasonably conclude that evidence of accessing the Target Website with the intention of viewing child pornography existed, and that this yielded a fair probability that evidence of criminality existed at the subject premises or on the computer the user of the Target IP address used to access the Target Website. See *Raymonda*, 780 F.3d at 116 (focusing on the defendant's purpose for visiting the site in drawing reasonable conclusions). This conclusion is supported by SA Fallon's representation that "a computer user's Internet activities generally leave traces or 'footprints' in the web cache and history files of the browser used." Fallon Aff. at ¶ 35(h).

#### **B. Staleness**

Defendant also argues that the Government's application was supported by only one alleged instance of an unstated duration of accessing a site affiliated with contraband images and provided no additional information from which a reviewing magistrate could infer that the targeted user had a predisposition toward child pornography. He contends that not only were the supporting facts deficient, but they were also too stale to form a basis for probable cause for a warrant that was sought seven months and eighteen days

(or 238 days) after the only alleged instance of the Target Website being accessed.

Again, Defendant raises an issue that presents a close question. However, although there is only one alleged instance of access to online child sexual abuse and exploitation material via the Target Website months before the warrant was sought, there was sufficient evidence alleged for Judge Stewart to reasonably conclude that there was a fair probability that evidence, fruits and instrumentalities of accessing the Target Website with the intent to view child pornography would be found at the Subject Premises and on the electronic devices located therein. As the Second Circuit stated in *Raymonda*, "courts have . . . inferred that a suspect was a hoarder of child pornography on the basis of a single incident of possession or receipt . . . where, for example, the suspect's access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files." *Raymonda*, 780 F.3d at 115. Here, although there is no evidence of a single incident of possession or receipt, there is evidence of a single episode of access to online child abuse and exploitation material which, as discussed, could reasonably mean access to child pornography. The evidence before Judge Stewart indicated that the user of the subject IP address went through a series of complicated steps to access the online child abuse and exploitation material on the Target Website, suggesting a deliberate intent to view images of child pornography available on that website. This provided a reasonable basis to conclude that the user of the subject IP address is a person interested in images of child pornography, that he or she accessed the website containing such images willfully and deliberately and not negligently or inadvertently, and that he or she actively sought out child pornography to satisfy a preexisting predilection. *See id.* Such circumstances support a reasonable inference that



the user of the subject IP address is a collector of child pornography likely to hoard such images in his or her home. See *id.* at 114-15. The evidence of the series of complicated steps the user of the subject IP address needed to take to access the online child sexual abuse and exploitation material via the Target Website distinguishes the instant case from the circumstances in *Raymonda* where the Second Circuit found insufficient a supporting affidavit indicating only a single incident of access to a site containing child pornography images without evidence of an affirmative step such as downloading or viewing full-sized files of child pornography. *Id.* at 116-17. The Second Circuit found that "[f]ar from suggesting a knowing and intentional search for child pornography, . . . the information in [the agent's] affidavit was at least equally consistent with an innocent user inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window." *Id.* at 117. Here, the complicated steps taken by the user of the subject IP address in order to access the online child sexual abuse and exploitation material on the Target website could reasonably be deemed as affirmative steps beyond mere inadvertent access. Furthermore, because of the incorporated difficulty in locating hidden services on Tor such as the Target Website, there was a reasonable basis to conclude that the user of the subject IP address actively sought out the Target Website and would have stored information related to the online directories and the Target Website on his electronic devices to access them more easily either on April 22, 2019 or thereafter.

### **3. Conclusion - Probable Cause**

For the reasons discussed above, the Court finds the totality of the allegations in SA Fallon's affidavit provided Judge Stewart a substantial basis to find that probable

cause existed to believe that evidence, fruits, and instrumentalities of a violation of 18 U.S.C. §§ 2252A(5)(B) and (b)(2) would be located at the Subject Premises and on computers and electronic devices located therein.

**b. Good Faith**

The Government argues that even if the search warrant was not supported by probable cause, law enforcement acted in good faith and therefore the evidence should not be suppressed. In opposition, Defendant argues that the good-faith exception to the exclusionary rule does not apply because SA Fallon demonstrated gross negligence by ignoring clearly established Second Circuit search and seizure law; the application so lacked indicia of probable cause that it was unreasonable to rely upon it; and SA Fallon recklessly provided misleading information to Judge Stewart by failing to include critical facts and making unsupported conclusions about the likelihood that evidence of criminality would be found at the location to be searched. The Court will examine each of Defendant's arguments in turn.

**1. Clearly Established Second Circuit Search and Seizure Law**

As Defendant argues, the Government has the burden to "demonstrate the objective reasonableness of the officers' good faith reliance on an invalidated warrant." *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011)(internal quotation marks and citation omitted). Citing to *Clark*, Defendant maintains that law enforcement officers cannot "claim reasonable reliance on warrants secured in the absence of compliance" with established legal precedent, *id.* at 105, and contends that "since *Falso* and *Raymonda* are clearly established controlling precedent and the same probable cause errors are

repeated here, the Government does not get the benefit of the good faith exception.” Dkt. 46-2 at 11. The Court disagrees with Defendant’s proposition underlying this argument.

Given the totality of the allegations asserted here, reasonable minds could differ whether the holdings of either *Falso* or *Raymonda* precluded a finding of probable cause in this case. In *Falso*, the supporting affidavit indicated only that it “appeared” that Falso had gained, or attempted to gain, access to the non-member section of a website that contained images of child pornography. See *Falso*, 544 F.3d at 120;<sup>12</sup> see also *id.* at 113;<sup>13</sup> *id.* at 114.<sup>14</sup> Here, by contrast, the supporting affidavit indicates that the FLA determined that the subject IP address had accessed child abuse and exploitation material on the Target website. Furthermore, in *Falso* the Second Circuit indicated that “[e]ven if one assumes (or infers) that Falso accessed the cpfreedom.com site, there is no specific allegation that Falso accessed, viewed or downloaded child pornography. While the non-member site contained approximately eleven images of child pornography, the affidavit lacks any information about whether the images were prominently displayed or required an additional click of the mouse; whether the images were downloadable; or what

---

<sup>12</sup> (“Falso’s case stands apart from those [cases] preceding it insofar as he was not alleged to have actually accessed or subscribed to any child-pornography website. Rather, Agent Lyons’s affidavit alleged only that Falso was perhaps one of several hundred possible subscribers to the cpfreedom.com website, who *appeared* either to have gained or attempted to gain access to the site. For this reason, *Martin* and *Coreas* are not controlling.”) (emphasis in original)

<sup>13</sup> (“Falso was not alleged to be a member or subscriber to a child-pornography website; it was alleged only that Falso ‘appeared’ to ‘have gained or attempted to gain’ access to a site that contained approximately eleven images of child pornography. Absent any allegation that Falso in fact accessed the website at issue, the question is whether Falso’s eighteen-year old conviction involving the sexual abuse of a minor (or some other factor) provides a sufficient basis to believe that evidence of child pornography crimes would be found in Falso’s home.”)

<sup>14</sup> (“The affidavit further stated that, based upon the FBI investigation and the forensic examination, ‘it appear[ed]’ that Falso ‘either gained access or attempted to gain access to the [non-member] website www.cpfreedom.com.’”)



other types of services and images were available on the site.” *Id.* at 121. Here, by contrast, reasonable minds could conclude that a sufficient basis existed for the conclusions that the primary purpose of the Target Website was to provide access to child pornography images, and that such images could be viewed and downloaded from the Target Website or from links provided thereat. For these reasons, it is a reasonable conclusion that *Falso*’s probable cause determination is distinguishable from the instant case, see *id.* at 121,<sup>15</sup> and does not compel the conclusion that probable cause was so lacking here that objectively reasonable officers could not believe in good faith that the warrant was legally supported.

The situation in *Raymonda* is also arguably distinguishable from the instant case. In *Raymonda*, the applying-agent’s “affidavit contained no evidence that the suspect downloaded any images of child pornography from [the website in issue], suggesting instead that the IP user did not even click on any thumbnail links to access the full-sized files.” *Raymonda*, 780 F.3d at 116. The Second Circuit found that “where the agents applied for a warrant on the basis of nine-month-old evidence, it was not enough simply to show that the suspect had at some point accessed thumbnails of child pornography. It was necessary to show that he accessed them in circumstances sufficiently deliberate or willful to suggest that he was an intentional ‘collector’ of child pornography, likely to hoard those images—or acquire new ones—long after any automatic traces of that initial incident

---

<sup>15</sup>(“In the end, the district court’s finding of probable cause in *Falso*’s case required it to make at least two significant additional inferential leaps not required in *Martin* and like cases. First, in *Falso*’s case there is no allegation that he in fact gained access to the *cpfreedom.com* website, much less that he was a member or subscriber of any child-pornography site. Second, there are no allegations to support an inference that the sole or principal purpose of the *cpfreedom.com* website was the viewing and sharing of child pornography, much less that images of child pornography were downloadable from the site.”)

had cleared.” *Id.* at 116-17. The Circuit found that probable cause was lacking where the agent’s affidavit “alleged only that, on a single afternoon more than nine months earlier, a user with an IP address associated with Raymonda’s home opened between one and three pages of a website housing thumbnail links to images of child pornography, but did not click on any thumbnails to view the full-sized files. The affidavit contained no evidence suggesting that the user had deliberately sought to view those thumbnails or that he discovered [the subject website] while searching for child pornography—especially considering that [the agent] himself only uncovered the website through an innocuous link on the message board of another site not explicitly associated with child pornography.” *Id.* at 117. The Circuit also found significant that there was no evidence that “the user subsequently saved the illicit thumbnails to his hard drive, or that he even saw all of the images, many of which may have downloaded in his browser outside immediate view.” *Id.* The Circuit indicated that “[f]ar from suggesting a knowing and intentional search for child pornography, in short, the information in [the agent’s] affidavit was at least equally consistent with an innocent user inadvertently stumbling upon a child pornography website, being horrified at what he saw, and promptly closing the window.” *Id.* The *Raymonda* Court found that “[u]nder those circumstances, absent any indicia that the suspect was a collector of child pornography likely to hoard pornographic files, . . . a single incident of access does not create a fair probability that child pornography will still be found on a suspect’s computer months after all temporary traces of that incident have likely cleared.” *Id.* Thus, the Circuit concluded, the warrant issued in that case was not supported by probable cause. *Id.*

The situation here arguably differs from that in *Raymonda*. The allegations in the supporting affidavit provide a reasonable basis to conclude that the user of the subject IP address accessed child abuse and exploitation material on the Target Website after undertaking a series of complicated steps to gain access, thus demonstrating efforts sufficiently deliberate or willful to suggest that the IP user “was an intentional collector of child pornography, likely to hoard those images—or acquire new ones—long after any automatic traces of that initial incident had cleared.” *Id.* at 116-117; *see also id.* at 115 (“In certain circumstances, courts have even inferred that a suspect was a hoarder of child pornography on the basis of a single incident of possession or receipt. They have done so where, for example, the suspect’s access to the pornographic images depended on a series of sufficiently complicated steps to suggest his willful intention to view the files.”). *Raymonda* does not necessarily compel the conclusion that probable cause was so lacking here that objectively reasonable officers could not believe in good faith that the warrant was legally supported.

Furthermore,

[a]s the Supreme Court has repeatedly stated, the exclusionary rule cannot be used to penalize law enforcement officers for a magistrate’s error. *See Leon*, 468 U.S. at 921, 104 S. Ct. 3405 (“Penalizing the officer for the magistrate’s error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.”); *see also [Davis v. United States]*, 564 U.S. 229, 246, 131 S. Ct. 2419, 180 L. Ed.2d 285 (2011)) (“[W]e have said time and again that the sole purpose of the exclusionary rule is to deter misconduct by law enforcement.”); *Massachusetts v. Sheppard*, 468 U.S. 981, 989-90, 104 S.Ct. 3424, 82 L.Ed.2d 737 (1984) (“[W]e refuse to rule that an officer is required to disbelieve a judge who has just advised him, by word and by action, that the warrant he possesses authorizes him to conduct the search he has requested.”). In *Leon*, for instance, the Supreme Court upheld the use of evidence collected in reliance on a search warrant that a magistrate judge had erroneously issued despite the absence of



probable cause. See 468 U.S. at 925-26, 104 S. Ct. 3405. The constitutional deficiencies of that warrant did not require exclusion of the evidence thereby obtained because the officers' reasonable reliance on the warrant did not implicate the deterrent purposes of the exclusionary rule.

*Eldred*, 933 F.3d at 120. Here, the alleged deficiencies in the warrant application are based upon legal authorities and conclusions that Judge Stewart presumably considered and found not to preclude issuance of the warrant. The executing officers should not be penalized for any error by Judge Stewart in issuing the warrant.

## 2. Indicia of Probable Cause Lacking

Next, Defendant argues that the warrant application so lacked indicia of probable cause that it was unreasonable to rely upon it. "*Leon* instructs that officers cannot reasonably rely on a warrant issued on the basis of an affidavit 'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'" *Clark*, 638 F.3d at 103 (quoting *Leon*, 468 U.S. at 923)(interior quotation marks and citations omitted). Showing such deficiency "is a very difficult threshold to meet." *Falso*, 544 F.3d at 128 n.24 (2d Cir. 2008). "Such a concern most frequently arises when affidavits are bare bones, *i.e.*, totally devoid of factual circumstances to support conclusory allegations." *Clark*, 638 F.3d at 103 (citations omitted). "The concern is particularly acute when facts indicate that the 'bare-bones description ... was almost calculated to mislead.'" *Id.* (quoting *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir.), *aff'd on reh'g*, 91 F.3d 331 (2d Cir.1996)). "In such circumstances, one *Leon* concern, *i.e.*, that 'a reasonably well trained officer would have known' that the challenged warrant was not supported by probable cause, is reinforced by another, *i.e.*, deception, or at least an apparent intent to deceive." *Id.* (quoting *Leon*, 468 U.S. at 922 n. 23).

At the opposite end of the spectrum are cases in which a defective warrant issued based on an affidavit providing detailed factual allegations in support of probable cause. Such cases almost invariably demonstrate reasonable reliance. As the Supreme Court explained in *Leon*, “[i]t is the magistrate’s responsibility to determine whether the officer’s allegations establish probable cause.... In the ordinary case, an officer cannot be expected to question the magistrate’s probable-cause determination....” *Id.* at 921, 104 S.Ct. 3405; accord *United States v. Falso*, 544 F.3d 110, 129 (2d Cir. 2008) (declining to hold that agents acted unreasonably in relying on judge’s probable cause determination because “the error ... was committed by the district court in issuing the warrant, not by the officers who executed it”); *United States v. Cancelmo*, 64 F.3d 804, 807 (2d Cir.1995)(holding that any error in issuance of warrant was “attributable to the magistrate who determined that the facts as alleged by the agents established probable cause”); *United States v. Thomas*, 757 F.2d 1359, 1368 (2d Cir.1985) (holding that, where magistrate, “whose duty it is to interpret the law,” determined that canine sniff could form basis for probable cause, “it was reasonable for the officer to rely on this determination”). The conclusion applies with particular force in circumstances where “thoughtful and competent judges” might disagree as to whether the facts alleged established probable cause. *United States v. Leon*, 468 U.S. at 926, 104 S.Ct. 3405; accord *United States v. Falso*, 544 F.3d at 128 (collecting cases).

*Clark*, 638 F.3d at 103–04.

Here, SA Fallon’s affidavit was not “bare bones,” but rather, as discussed above, provided detailed factual allegations in support of probable cause. *See, e.g., United States v. Safford*, 814 F. App’x 638, 641 (2d Cir. 2020)(“Far from being bare-bones, the application and affidavit here detailed several objective facts supporting the existence of probable cause to believe that anyone who logged into Playpen did so intending to view or trade child pornography.”). While thoughtful and competent judges might disagree as to whether the alleged facts established probable cause, it was reasonable for the executing officers to rely on Judge Stewart’s probable cause determination in executing the warrant. Based on the allegations in the application and supporting affidavit, the Court “cannot say

that the warrant was 'so lacking in indicia of probable cause' that an officer would have 'no reasonable grounds' to believe the warrant was properly issued." *Id.* (quoting *Leon*, 468 U.S. at 923 (internal quotation marks omitted)).

### **3. Recklessly Providing Misleading Information**

Next, Defendant argues that the good-faith exception is not applicable because SA Fallon recklessly provided misleading information to Judge Stewart by failing to include critical facts and making unsupported conclusions about the likelihood that evidence of criminality would be found at the location to be searched. In his motion, Defendant asserts that SA Fallon "recklessly mislead the magistrate with his application" as to whether there was probable cause to search the Defendant's residence and electronic devices. In this regard Defendant asserts that because of the "glaring deficiencies" in SA Fallon's affidavit that Defendant challenges in his motion, "SA Fallon[] made baseless, conclusory representations that there was probable cause to search the Defendant's residence and electronic devices." Dkt. 46-2 at 12. In his Reply, Defendant indicates that he "agrees that a *Franks* hearing is not necessary as there is no issue of fact that needs resolution or amplification from an evidentiary hearing." Dkt. No. 58 at 7. He indicates that he "is not and has not made any claim that SA Fallon intentionally mislead the court, only that he was reckless in his application by ignoring well established controlling law as described above and not including anywhere near the facts necessary to establish probable cause." *Id.* Defendant's conclusory contentions, and his general disagreement with Judge Stewart's probable cause determination, do not demonstrate that the executing officers did not reasonably rely in good faith on Judge Stewart's determination. As indicated



above, while reasonable minds might disagree with Judge Stewart's determination, the supporting affidavit was not so lacking detailed allegations supporting probable cause that it was unreasonable for the executing officers to rely on Judge Stewart's determination in issuing the warrant.

Defendant also contends that SA Fallon "made it appear as though the user of the Defendant's IP address had registered for an account with the Target Site" by including facts related to what a user could do, user data and images trafficked by users, and that he misled Judge Stewart by failing to indicate that the Government was not in possession of evidence showing that the Target IP Address user was a registered user of the Target Website. However, when put in the context of the full affidavit, Defendant's contention is without merit. SA Fallon included the user information cited by Defendant in the section of the affidavit where he described the Target Website. See Fallon Aff., ¶¶ 15-18. This appeared to be a description of the Target Website in general, not as it was used or accessed by the Target IP Address user. See *id.* That section is separate from the next section titled, in bold, "Evidence Related to Identification of Target that Accessed Target Website." *Id.* at p. 13. In the latter section, which focuses on the actions of the Target IP Address user, SA Fallon includes information as to what users with and without an account could access. See *id.* at ¶ 20. Nowhere in the affidavit did SA Fallon claim that the Target IP Address user is a registered user of the Target Website, nor did he ask the Court to reach that conclusion. The Government indicates that SA Fallon could not make that representation because the FLA did not provide registration or account information to the FBI. However, as the Government argues, failing to state that such evidence was not

provided to the FBI was not a knowing or reckless omission that would mislead Judge Stewart. Rather, a common-sense conclusion drawn from the affidavit would be that the FBI was not in possession of such evidence and information, because if it was, it would have included it in the affidavit. Also as the Government contends, SA Fallon provided an accurate recitation of the facts and Judge Stewart was at liberty to draw his own conclusions based on those facts.

Defendant also claims that SA Fallon misled Judge Stewart by failing to indicate that the Target IP Address was not registered with the National Center For Missing and Exploited Children ("NCMEC") or the Internet Crimes Against Children (ICAC) Child Online Protection System, Def. Ex. D at 4, and by failing to indicate that it was determined that Defendant had no prior criminal history, was not a registered sex offender, and that FBI database searches "did not identify any derogatory information" about Defendant. *Id.* at pg. 5. "[T]o assert good faith reliance successfully, officers must, *inter alia*, disclose all potentially adverse information to the issuing judge." *United States v. Ganas*, 824 F.3d 199, 221 (2d Cir. 2016)(citing *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996) ("The good faith exception to the exclusionary rule does not protect searches by officers who fail to provide all potentially adverse information to the issuing judge...."), *aff'd and amended*, 91 F.3d 331 (2d Cir. 1996) (*per curiam*)). Defendant contends that the omission of evidence showing no connection between the subject IP address and the NCMEC or the ICAC Child Online Protection System, and the omission of evidence showing no connection between Defendant and any prior criminal or child abuse history, is adverse to SA Fallon's statement at ¶ 6 of his affidavit that a "user of the Internet account

at the SUBJECT PREMISES has been linked to an online community of individuals who regularly send and receive child pornography” and that “there is probable cause to believe that a user of the Internet account at the SUBJECT PREMISES accessed the TARGET WEBSITE as further described herein.” See Dkt. No. 46-2 at 12; see *also* Dkt. No. 58 at 7 (“Since none of this information (which is adverse to . . . SA Fallon’s representation that . . . the Defendant was linked to a child sexual exploitation website) was made known to the court, the Government does not get the benefit of the good faith exception.”). Defendant’s argument in this regard does not defeat application of the good-faith exception to the exclusionary rule. A review of the totality of the allegations reveals that the subject IP address was linked to the Target Website by the FLA’s determination based upon its independent investigation that the subject IP address had accessed online child sexual abuse and exploitation material via the Target Website on April 22, 2019, not because the subject IP address or Defendant had some prior involvement with child abuse or child pornography. Thus, in this regard the omission of the information referenced by Defendant was not material to the determination that the subject IP address was linked to the Target Website. While it may have been material to whether Defendant or some other user of the subject IP address was interested in child pornography and potentially maintained evidence of that interest nearby, this conclusion here is not supported by prior involvement with child abuse and child pornography but rather by the series of complicated steps taken to access the Target Website. Indeed, the lack of prior involvement does not necessarily mean that probable cause could not exist because even someone without prior brushes with the law could have a proclivity to hoard child pornography nearby. Further, as the Government argues, Judge Stewart likely was not



mislead because common sense would seemingly lead Judge Stewart to conclude that because relevant child abuse and criminal history was not provided, such history did not exist. For these reasons, application of the good-faith exception to the exclusionary rule will not be denied on this basis.

Finally, Defendant contends that SA Fallon mislead Judge Stewart by including “pages of boilerplate information about child pornography cases, predilections of past offenders and use of the internet and the Tor program that have *nothing to do with the Defendant* or his IP address.” Dkt. 46-2 at 13 (emphasis in original). Defendant cites to Judge Chin’s separate opinion in *Raymonda* for the proposition that “it is ‘inappropriate-and heedlessly indifferent’ for an agent to ‘rely on boilerplate language regarding the proclivities of collectors’ when there is no evidence that the Defendant or the Defendant’s IP address are actually involved in the collection of child pornography.” *Id.* (quoting *Raymonda*, 780 F.3d at 124 (Chin, J. concurring in part and dissenting in part)). Here, however, and as discussed above, the alleged facts - including that the user of the Subject IP address accessed online child abuse and exploitation material on the Target Website and that, to do so, had to go through a complex series of steps - provide a basis to conclude that the user of the subject IP address exhibited characteristics consistent with a collector of child pornography. Thus, evidence exists upon which to conclude that SA Fallon did not recklessly mislead Judge Stewart by providing boilerplate language about the proclivities of collectors of child pornography.

#### **4. Conclusion - Good-Faith Exception**

For the reasons discussed above, assuming *arguendo* that the warrant was

improperly issued, SA Fallon and the other officers who executed that warrant are entitled to the good-faith exception to the exclusionary rule.

**c. Defendant's Statements**

Inasmuch as the Court finds that the warrant was properly executed either because probable cause existed and the evidence sought to be discovered was not stale, or because the officers relied in good faith on Judge Stewart's determination, Defendant's argument seeking to suppress his statements as the product of an unconstitutional warrant is without merit. Without other meritorious grounds advanced for the suppression of Defendant's statements, this aspect of Defendant's motion is denied.

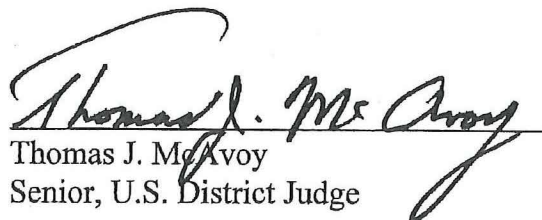
**V. CONCLUSION**

For the reasons discussed above, Defendant's motion to suppress physical evidence seized from his residence, computers, and electronic storage media, and to suppress all statements obtained during and after the search, Dkt. No 44, is **DENIED**.

The parties are directed to consult with each other and, within two (2) weeks from the date of this Decision and Order, present to the Court a jointly-agreed upon proposed redacted Decision and Order that does not disclose information that might jeopardize the Government's continuing investigations but that also satisfies the governing legal standard for public access to court documents discussed in *Lugosch v. Pyramid Co. of Onondaga County*, 435 F.3d 110, 119-27 (2d Cir. 2006).

**IT IS SO ORDERED.**

Dated: July 19, 2021

  
Thomas J. McAvoy  
Senior, U.S. District Judge